Amendments to the Claims

1-4. (canceled)

5. (previously presented) The cryptography engine of claim 71, wherein the third bit sequence is less than 32 bits.

6. (previously presented) The cryptography engine of claim 71, wherein the third bit sequence is four bits.

7. (previously presented) The cryptography engine of claim 5, wherein the first bit sequence is less than 48 bits.

8 . (previously presented) The cryptography engine of claim 6, wherein the first bit sequence is less than six bits.

9-10. (canceled)

11. (previously presented) The cryptography engine of claim 68, wherein the fourth bit sequence is less than 32 bits.

12. (previously presented) The cryptography engine of claim 68, wherein the fourth bit sequence is four bits.

13. (previously presented) The cryptography engine of claim 68, further comprising a multiplexer circuitry including a two-level multiplexer.

14. (previously presented) The cryptography engine of claim 13, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer.

15. (canceled)

16. (previously presented) The cryptography engine of claim 68, wherein the key scheduler performs pipelined key scheduling logic.

17. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a determination stage.

18. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a shift stage.

19. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a propagation stage.

20. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a consumption stage.

21. (previously presented) The cryptography engine of claim 17, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

22-47. (canceled)

48. (previously presented) The integrated circuit layout of claim 76, wherein the first bit sequence is four bits.

49. (previously presented) The integrated circuit layout of claim 48, wherein the expanded first bit sequence is less than six bits.

50. (previously presented) The integrated circuit layout of claim 73, wherein the key scheduler performs pipelined key scheduling logic.

51. (previously presented) The integrated circuit layout of claim 73, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

52. (previously presented) The integrated circuit layout of claim 51, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

53. (previously presented) The integrated circuit layout of claim 73, further comprising a multiplexer circuitry including a two-level multiplexer.

54. (previously presented) The integrated circuit layout of claim 53, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer.

55-67. (canceled)

68. (previously presented) A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

means for combining via a first logical operation one of the plurality of keys provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block;

substitution logic for receiving the second bit sequence and for generating a third bit sequence;

a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logic operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and

a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

69. (previously presented) The cryptography engine of claim 68, wherein the first and second logical operations are binary XOR operations.

70. (previously presented) The cryptography engine of claim 68, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

71. (previously presented) The cryptography engine of claim 70, wherein the third bit sequence is less than the first bit sequence.

72. (previously presented) The cryptography engine of claim 68, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

73. (previously presented) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the integrated circuit layout comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

means for combining via a first logical operation one of the plurality of keys provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block;

substitution logic for receiving the second bit sequence and for generating a third bit sequence;

a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logical operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and

a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

74. (previously presented) The integrated circuit layout of claim 73, wherein the first and second logical operations are binary XOR operations.

75. (previously presented) The integrated circuit layout of claim 73, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

76. (previously presented) The integrated circuit layout of claim 73, wherein the second bit sequence is less than the first bit sequence.

77. (previously presented) The integrated circuit layout of claim 73, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

78. (previously presented) A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

an expansion logic for expanding the first portion of the data block and for generating a first bit sequence having a first bit size;

a first XOR logic for performing a first XOR operation of a first key provided by the key scheduler and the first bit sequence and for generating a second bit sequence;

an Sbox logic for taking the second bit sequence and for generating a third bit sequence having a second bit size smaller than the first bit size;

a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

a second XOR logic performing a second XOR operation of the third bit sequence and the second inverse permuted bit sequence to generate a fourth bit sequence; and

a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

79. (previously presented) The cryptography engine of claim 78, wherein the data block contai9ns bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

80. (withdrawn) A method for performing an accelerated multiple round cryptographic operation in a cryptographic engine having performance and expansion logic in a non-timing critical path, comprising:

performing an initial cryptographic round, wherein the step of performing the initial cryptographic round includes:

determining an inverse permutation of a first portion of an input sequence, wherein the first portion of the input sequence is set as a left portion of an input bit sequence for the initial round,

determining an inverse permutation of a second portion of the input sequence, wherein the second portion of the input sequence is set as the right portion of the input bit sequence for the initial round,

expanding the first portion of the input sequence to generate an expanded first portion,

exclusively ORing the expanded first portion with an initial round key generated by a key scheduler to generate a first bit sequence,

transforming the first bit sequence to a second bit sequence using a substitution box, exclusively ORing the second bit sequence with the left portion of the input bit sequence for the initial round to generate a right portion of an output bit sequence for the initial round; and

performing a subsequent cryptographic round, the step of performing the subsequent cryptographic round includes:

receiving the right portion of the input bit sequence of the initial round and selecting the right portion of the input bit sequence of the initial round as the left portion of an input bit sequence of the subsequent round,

determining the permutation of the right portion of the output bit sequence of the previous cryptographic round, wherein the result of the permutation is a third bit sequence,

expanding the third bit sequence to generate an expanded third bit sequence,

exclusively ORing the expanded third bit sequence with a round key for the subsequent cryptographic round to generate a fourth bit sequence,

transforming the fourth bit sequence to a fifth bit sequence using the substitution box,

exclusively ORing the fifth bit sequence with the left portion of the input bit sequence for the current round to generate a right portion of an output bit sequence for the subsequent cryptographic round.